IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI

IN THE MATTER OF THE APPLICATION	**)**	
OF THE UNITED STATES OF AMERICA FOR	**)**	
AN ORDER FOR AUTHORIZATION TO	**)**	**No. 3:15MC3**
OBTAIN LOCATION DATA CONCERNING AN	**)**	
AT&T CELLULAR TELEPHONE	**)**	**(SEALED)**

ORDER

This cause comes before the court on the motion of the government, appealing the Magistrate Judge's denial of its application for a warrant, pursuant to 18 U.S.C. § 2703(c)(1)(A) of the Stored Communications Act (SCA), which sought to compel the disclosure of cell phone records to be used as part of an ongoing drug trafficking investigation in this district. The warrant which the government sought to obtain was a "prospective" one, which would have compelled phone providers to provide cell phone location data to be generated in the future, which the government intended to use to track the location of drug suspects. The government's application in this regard gives rise to a number of difficult Fourth Amendment and statutory interpretation issues, and, in the absence of binding U.S. Supreme Court precedent on point, this court can only give its best guess regarding what the law in this context actually is. With that caveat, this court, having considered the briefing of the government and that of the Federal Public Defender as *amicus curiae*, concludes that the government's appeal is well taken and should be sustained, for reasons which it will presently explain.

The issues in this case are, it appears, an inevitable result of advances in cell phone technology, which seem to have outpaced the legal standards to deal with them. The government

has filed applications similar to this one in a large number of jurisdictions nationwide, thereby giving rise to a significant, and divergent, body of case law on this subject. In her February 10, 2015 order denying the government's application for a warrant, Magistrate Judge Alexander found persuasive and expressly relied upon a 2014 order by U.S. Magistrate Judge William Smith, of the Southern District of Texas, in *In the Matter of the Application of the United States of America for an ORDER AUTHORIZING PROSPECTIVE AND CONTINUOUS RELEASE OF CELL SITE LOCATION RECORDS*, 31 F. Supp. 3d 889 (S.D. Tex. 2014).

In particular, Judge Alexander relied upon Judge Smith's ruling that, when prospective (rather than historical) cell phone location data is sought by the government, it is required to proceed under the Tracking Device Statute, 18 U.S.C. § 3117, rather than the SCA. In Judge Smith's case, however, the government sought an "order" under § 2703(d) of the SCA, which is an entirely different SCA provision than the one the government uses in this case, and one which imposes a "specific and articulable facts" standard that requires a considerably lesser showing of proof than the probable cause standard to which the government has agreed to subject itself here. This is significant since, while Judge Smith wrote that his analysis applied regardless of "[w]hether or not cell site data is ultimately held worthy of Fourth Amendment protection,"*In the Matter of the Application*, 31 F. Supp. 3d at 900, he approvingly cited and appeared to tacitly rely upon a 2005 decision in which he wrote that "permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected." *In Re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005).

In his 2014 decision, Judge Smith appeared reluctant to re-state his earlier view that the government's use of cell phone data implicates Fourth Amendment protection, perhaps in recognition of the fact that a number of federal courts have, since his 2005 decision was written, reached a contrary conclusion. In so noting, this court emphasizes that the U.S. Supreme Court has not yet clarified exactly what Fourth Amendment protection, if any, exists when the government seeks to obtain physical location data generated by a suspect's cell phone. In *United States v. Jones*, 132 S. Ct. 945, 949, 181 L. Ed. 2d 911 (2012), the Supreme Court did hold that the attachment of a GPS tracking device to a vehicle without the owner's permission was a "search" within the meaning of the Fourth Amendment. *Jones* does not resolve the Fourth Amendment issues arising from applications for cell phone location data, however, since its rationale was expressly based upon the physical placement of a tracking device on a suspect's car, which the Supreme Court found "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Jones*, 132 S. Ct. at 949.

In the absence of relevant U.S. Supreme Court authority, lower federal courts have analyzed the constitutional issues in this context in different ways. There is, however, broad agreement that those issues should be analyzed under the Fourth Amendment standard set forth by the U.S. Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967) and its progeny, which deem a Fourth Amendment violation to have occurred when government officers violate a person's "reasonable expectation of privacy." *See also Bond v. United States*, 529 U.S. 334, 120 S. Ct. 1462, 146 L. Ed. 2d 365 (2000). What those words actually mean in their application to cell phone tracking data is very much in dispute, however. A number of federal courts have concluded that there is no reasonable expectation of privacy in location data emanating from one's cell phone, while others have disagreed and concluded that when the government seeks to

obtain such data from cell phone providers it must demonstrate probable cause and obtain a warrant. This court will first discuss select cases adopting the former view.

In *United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012), the Sixth Circuit Court of Appeals held that a defendant convicted of drug running "did not have a reasonable expectation of privacy in the GPS data and location of his cell phone" while traveling on public thoroughfares and accordingly affirmed his conviction based on location data from his phone. In *Skinner*, law enforcement officers tracked the defendant's phone for three days while he transported drugs on public highways, utilizing an order from a magistrate judge which authorized prospective, real-time monitoring of the location data from his phone. *Skinner*, 690 F.3d at 776. In concluding that he had no reasonable expectation of privacy in that prospective cell phone data, the Sixth Circuit wrote that:

> When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them. This is not a case in which the government secretly placed a tracking device in someone's car. The drug runners in this case used pay-as-you-go (and thus presumably more difficult to trace) cell phones to communicate during the cross-country shipment of drugs. Unfortunately for the drug runners, the phones were trackable in a way they may not have suspected. The Constitution, however, does not protect their erroneous expectations regarding the undetectability of their modern tools.

Id. at 774. The Sixth Circuit further stressed that the three-day monitoring of the defendant's location was a limited one, and it acknowledged concerns expressed by Justice Alito in his concurring opinion in *Jones* (joined by three other Justices), 132 S. Ct. at 957–64, that a lengthy surveillance might well violate a defendant's reasonable expectation of privacy. *Id.* at 780.

Other federal courts, in reaching similar results, have found that no reasonable expectation of privacy existed based upon the so-called "third party disclosure doctrine" set forth by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 740, 99 S. Ct. 2577 (1979). In *Smith*, the Supreme Court held that there was no reasonable expectation of privacy in dialing information gleaned from pen registers, concluding that telephone users were aware that phone companies (1) had facilities for recording phone numbers, and (2) did in fact record that information for legitimate business purposes. 442 U.S. at 742.

In *U.S. v. Booker*, 2013 WL 2903562 (N.D. Ga. 2013), a Georgia district judge deemed the *Smith* analysis as controlling in the cell phone location data context, writing that:

> Similarly, today, mobile telephone users sufficiently understand that the cell phone company (1) has facilities for recording the cellular tower information employed in dialing a number, and (2) does in fact record that information for legitimate business purposes, such as billing different rates when the customer is "roaming." . . . Accordingly, the cell phone user assumes the risk that the company could reveal that legitimate business information to others, including law enforcement authorities, as part of an investigation. *See Smith*, 442 U.S. at 744. As the Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily conveys to third parties" any expectation of privacy defendants assert in cell site location information contained in cell phone company records "is not one that society is prepared to recognize as reasonable" and as such, the information is not protected by the Fourth Amendment. *Id.* at 743–44.

Booker, 2013 WL 2903562 at 9. Citing a number of decisions from other district courts reaching a similar conclusion,[1] the Georgia court declined to suppress tracking data which had been

[1]*See, e.g. United States v. Benford*, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. 2010) ("[D]efendant had no legitimate expectation of privacy in records held by a third-party cell phone company identifying which cell phone towers communicated with defendant's cell phone at particular points in the past."); *In re Application of the U.S. for an Order Authorizing the Disclosure of CellSite Location Info.*, No. 6:08–6038M–REW, 2009 WL 8231744, at *10 (E.D. Ky. 2009) ("[A] cell phone user that places or receives a call knows that he or she is participating in and relying on the cell provider's network and switching equipment. Indeed, the very act of connection-including cell site activations—requires participation, by the user, in the facilities

obtained based on § 2703(d)'s "specific and articulable facts" standard, pursuant to an order from a Magistrate Judge which provided for prospective monitoring of cellular site location data for a period of sixty days. The Georgia district court rejected the argument that the SCA was inapplicable to applications for prospective cell data, finding that "[t]he SCA makes no distinction between historical and prospective cell site location information." *Id.* at 6.

In a 2-1 split panel decision in *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013), the Fifth Circuit held that the use of § 2703(d)'s "specific and articulable facts" standard, rather than a Fourth Amendment probable cause standard, was not *per se* unconstitutional, in cases where the government sought to compel cell phone service providers to produce historical cell site information. In rejecting the arguments of the ACLU as *amicus curiae* to the contrary, the Fifth Circuit wrote that:

> [T]o obtain an order for the historical cell site records of a particular cell phone owner, the Government may apply to a court that has jurisdiction. And that court must grant the order if the Government seeks an order (1) to "require a provider of electronic communication service or remote computing service" (2) "to disclose a [non-content] record or other information pertaining to a subscriber to or customer of such service" when the Government (3) meets the "specific and articulable facts" standard. If these three conditions are met, the court does not have the discretion to refuse to grant the order.

In re Application of the U.S., 724 F.3d at 607.

In his 2014 opinion, Judge Smith noted the Fifth Circuit's decision in *In re Application of the U.S.*, but he emphasized that it was based on *historical* phone records and he appeared to conclude that its analysis would not be applied in cases seeking prospective cell phone data. *In*

---

provided by the particular company for the purpose of call completion."); *U.S. v. Suarez-Blanca*, 2008 WL 4200156, *9 (N.D. Ga. 2008)("[I]n dialing certain numbers, the defendants ... voluntarily agreed to turn over information about which towers were used in placing those calls."); *United States v. Perez–Alonzo*, No. CRIM.03–221(1), (2) A, 2003 WL 22025863, at *2

the Matter of the Application, 31 F. Supp. 3d. at 891-92. While Judge Smith may prove to be correct in this regard, this court has its doubts. Although limited to cases of historical cell phone location data, this court views *In re Application of the U.S.* as being broadly supportive of law enforcement concerns in *all* cell phone location data contexts. Indeed, the panel majority's opinion raises many of the same arguments which have repeatedly surfaced in decisions approving applications for both historical and prospective cell phone data. For example, the panel majority appeared to endorse, in the historical data context, the application of the same "third party disclosure" doctrine which a number of federal decisions, discussed above, have applied to applications for prospective cell phone location data. Specifically, the Fifth Circuit wrote that:

> Therefore, the Government, when determining whether an intrusion constitutes a search or seizure, draws a line based on whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information. Where a third party collects information in the first instance for its own purposes, the Government claims that it can obtain this information later with a § 2703(d) order, just as it can subpoena other records of a private entity. Compare *Smith v. Maryland*, 442 U.S. 735, 743, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979) (finding significant that "the phone company does in fact record this information for a variety of legitimate business purposes " (emphasis added)), with *United States v. Jones*, 132 S. Ct. 945, 964, 181 L.Ed.2d 911 (2012) (Alito, J., concurring in the judgment) (expressing concern over the application of existing Fourth Amendment doctrine to "the use of GPS tracking technology for law enforcement purposes " We agree.

Id. at 610.

The Fifth Circuit in *In re Application of the U.S.* advanced other arguments which have frequently been expressed in cases seeking prospective cell phone data, such as that "[a] cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a

---

(D. Minn. 2003) (holding that the defendant had no reasonable expectation of privacy in his

nearby cell tower in order to wirelessly connect his call" and that the "use of their phones, moreover, is entirely voluntary." *Id.* at 613. Moreover, in quite broad language, the logic of which seems to apply in the prospective cell phone data context, the Fifth Circuit wrote that:

> We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, *Greenwood*, 486 U.S. at 40–41, 108 S.Ct. 1625, or the view of their property from 400 feet above the ground, *Florida v. Riley*, 488 U.S. 445, 451, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only *reasonable* expectations of privacy.

Id. at 615. Thus, there is clearly binding Fifth Circuit precedent finding that there is no reasonable expectation of privacy in historical cell phone data, and this court doubts that prospective cell phone data is sufficiently different from historical cell phone data to warrant a different result.

It seems to this court that, both as a practical matter and as a constitutional matter, there is no great distinction between historical and prospective cell phone location data. As a practical matter, a number of federal courts have found persuasive the "instantaneous storage theory," which recognizes that, in the digital age, prospective data instantly becomes stored data, as soon as it is transmitted to a cell phone provider's servers. *See United States v. Booker*, 2013 WL 2903562, *7 (N.D. Ga. June 13, 2013) ("While this information is 'prospective' in the sense that the records had not yet been created at the time the order was authorized, it is no different in substance from the historical cell site information ... at the time it is transmitted to the government."); *In re Application*, 632 F. Supp. 2d 202, 207 n. 8 (E.D. N.Y. 2008) (Garaufis) ("The prospective cell-site information sought by the Government ... becomes a 'historical

---

mobile phone records).

record' as soon as it is recorded by the provider."); *In re Application*, 460 F. Supp. 2d 448, 459 (S.D. N.Y. 2006) (Kaplan) ("[T]he information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials."); *In re Application*, 405 F. Supp. 2d 435, 444 (S.D. N.Y. 2005) (Gorenstein) (nothing in the SCA limits when "information may come into being").

As a constitutional matter, it is not clear to this court that a defendant has a significantly different expectation of privacy with regard to historical cell phone location data than he does with regard to prospective cell phone data. This is particularly true when the monitoring of prospective data is only for a limited duration, thereby addressing the concerns expressed in Justice Alito's concurrence in *Jones*. In so concluding, this court notes that the U.S. Supreme Court's Fourth Amendment jurisprudence has generally regarded an individual's expectation of privacy as being strongest in relation to his home. *U.S. v. Karo*, 468 U.S. 705, 714 104 S.Ct. 3296 (1984). ("[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.") In this vein, it appears significant to this court that historical, and not prospective, cell phone data would be most useful to the government in ascertaining the location of a suspect's home. It seems to this court that, if the government wanted to ascertain the location of a suspect's home, its best bet would be to obtain his historical cell phone data and simply ascertain the location to which he returns each night.

It seems clear enough that prospective cell phone data is most useful to the government in cases where a suspect is actively moving from location to location, such as in *Skinner*'s scenario involving a drug trafficker traveling to a drug buy. In such a scenario, it must be asked whether

the defendant actually has a more reasonable expectation of privacy regarding his location than when he is in the privacy of his home. This court has serious doubts that he does, particularly since, in traveling to the drug transaction, he would be utilizing public highways and exposing himself to public view. If a less-than-saavy defendant chooses to travel to a drug buy while carrying a cell phone which is turned on and thus sending out location data to cell towers owned by third parties, does he truly have a reasonable expectation of privacy in that data? A number of federal courts have concluded that he does not, and this court is inclined to agree with them.

Other federal courts have disagreed with the above analysis, concluding that cell phone tracking data does, in fact, implicate a defendant's reasonable expectation of privacy and is entitled to Fourth Amendment protection. In *In re App. of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device,* 396 F. Supp. 2d 294 (E.D. N.Y. 2005), for example, a New York Magistrate Judge approvingly cited Judge Smith's 2005 decision for the proposition that:

> Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge.

In re App., 396 F. Supp. 2d at 322-23, *citing In Re Application*, 396 F. Supp. 2d at 756. The New York Magistrate Judge thus agreed with Judge Smith's view that the "third party disclosure doctrine" set forth in *Maryland v. Smith* was inapplicable to cell phone location data, a conclusion with which, as noted above, a number of federal judges have disagreed.

Once again, Judge Smith wrote in his 2014 opinion that the Tracking Device Statute was the proper one to obtain prospective cell phone data regardless of whether it enjoys Fourth Amendment protection, but this court cannot help but believe that his analysis was, at least

tacitly, influenced by his previously-stated view that such data does, in fact, enjoy such protection and that the SCA is insufficient to provide it. And, indeed, if Judge Smith's previously-stated view that prospective cell phone data enjoys Fourth Amendment protection is correct, then the SCA provision at issue in his case *is* likely insufficient to provide it. Specifically, the SCA provision at issue in Judge Smith's case, § 2703(d), provides that:

> (d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Section § 2703(d)'s basic standard thus requires a showing of "specific and articulable facts," which all parties agree presents a considerably lesser burden of proof on the government than the probable cause standard does.

It further appears to this court that Judge Smith's references to the "SCA" in his opinions are often best regarded as references to § 2703(d), and he frequently seemed to equate a decision to proceed under the SCA with a decision to proceed under a less exacting burden of proof. In his 2005 opinion, Judge Smith framed the issue before him as follows:

> The issue presented here is what legal standard the government must satisfy to compel disclosure of such prospective or "real-time" cell site data. More particularly, is this location information merely another form of subscriber record accessible upon a showing of "specific and articulable facts" under 18 U.S.C. § 2703(d), as the government contends? Or does this type of surveillance require a more exacting standard, such as probable cause under Federal Rule of Criminal Procedure 41?

In Re Application, 396 F. Supp. 2d at 749. In his 2014 decision, Judge Smith appeared to regard a decision to proceed under the SCA as tantamount to a decision to forego seeking a warrant based on probable cause, writing that:

> Writing on a mostly clean slate nine years ago, this court concluded that prospective monitoring of cell site data converts a cell phone into a "tracking device" under the federal Tracking Device Statute, which is subject to the warrant requirements of Rule 41 of the Federal Rules of Criminal Procedure. Since 2005, other magistrate and district judges have weighed in. Some disagreed that a warrant was necessary, holding that such prospective location data is available under the lower, "specific and articulable facts" threshold of the SCA.

Id. at 891. In summarizing his view that the SCA was inapplicable, Judge Smith similarly wrote that:

> These considerations compel me to respectfully disagree with my colleague from New York, and to reject the SCA as stand-alone authority for prospective, continuous, and contemporaneous cell site monitoring. Both in fact and in law, this type of surveillance converts a smartphone into a tracking device, and it is governed by the standards of Rule 41, not the SCA.

Id. at 899.

Thus, Judge Smith seemed to frame the issues before him as an "either/or" proposition, in which the government either establishes probable cause under the Tracking Device Statute or proceeds under the SCA and its "specific and articulable facts" standard. The facts here demonstrate that this is not necessarily the case, however. It appears to this court that, inasmuch as § 2703(d) is the SCA provision which has actually been utilized by the government in most cases, it has come to be regarded by many federal judges as something of a shorthand for the SCA itself. This is understandable, since the SCA's provision, in § 2703(c)(1)(A), for a warrant based upon probable cause is of no great significance if the government never actually uses it. The government *has* chosen to utilize § 2703(c)(1)(A) in this case, however, and this court believes that this fact highlights that the SCA is actually a much more flexible and workable statute for obtaining cell phone data, both historical and prospective, than Judge Smith seemed to believe.

In analyzing Congress's intent in drafting the SCA, it seems appropriate to analyze the language which it actually drafted, regardless of how it has subsequently been used by many prosecutors. The language which Congress actually drafted in the SCA strikes this court as being quite flexible, providing options for both "warrants" and "orders" which will seemingly accommodate any constitutional interpretations which might be forthcoming from the federal courts. Specifically, § 2703(c) of the SCA provides that:

> (c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
>
> (B) obtains a court order for such disclosure under subsection (d) of this section;

Once again, the government has chosen to utilize § 2703(c)(1)(A)'s option for a warrant based upon probable cause in this case, and it seems to this court that, in so doing, it has given the Magistrate Judge the discretion to fashion a warrant which accounts for both the practical needs of this case and any constitutional concerns which might exist in this context.

For example, it appears to this court that Judge Alexander might reasonably (and likely should) set a specific duration for any prospective cell phone data surveillance she authorizes under § 2703(c)(1)(A), to address the concerns expressed by Justice Alito in *Jones*. Such a limited duration would also help address some of the concerns raised by Judge Smith in his 2014 order, where he noted that "[t]he SCA has no monitoring periods, no extensions, no minimization requirements, no periodic reporting, no automatic sealing. In short, none of the signature elements of an ongoing surveillance scheme are present." *Id.* at 895. While it is true

that the SCA has no such specific limitations, this court does not read the statute, or Rule 41, as *forbidding* a Magistrate Judge from setting such limitations herself, in any warrant she issues. Such would seemingly be more effective than an approach based upon the Tracking Device Statute, which was designed to deal with physical "installation" of tracking devices rather than requests for data from third party cell phone providers, which is clearly within the SCA's "wheelhouse."

In this court's view, the Supreme Court's recent decision in *Jones*, discussed previously, suggests that the "installation" language in the Tracking Device Statute constitutes a real reason for not utilizing that statute for requests for prospective cell phone location data.[2] In concluding otherwise, Judge Smith wrote in his 2014 opinion that "an 'installation' in our digital age need not entail a physical process, like placing a beeper under a truck bumper; as often as not the term refers to a screen tap or keystroke by which new software is electronically 'installed' on digital devices." *Id.* at 898. In *Jones*, however, the Supreme Court *did* regard the physical installation of a tracking device on a vehicle as being the key factor which rendered it a "search," based upon notions about the nature of searches at the time the Fourth Amendment was enacted. *Jones*, 132 S. Ct. at 949. This analysis is obviously inapplicable to cell phone location data tracking. It thus appears that the Fourth Amendment analyses applicable to tracking devices and applications for prospective cell phone location data are heading in different directions, and this constitutes, in this court's view, additional reason for not tethering them together in the same enforcement statute.

[2]18 U.S.C. § 3117(a) provides that "[i]f a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction."

Moreover, the very fact that, in this case, the government has argued so forcefully in favor of applying the SCA rather than the Tracking Device Statute, after agreeing to be bound by similar constitutional standards under either, in and of itself lends credibility to its argument that the SCA is better suited to meet the practical needs of requests for cell phone data. Indeed, this court can discern no good reason why it would make this argument if such were not its genuine motivation, since the constitutional standards it faces will be very similar, if not identical, regardless. In its brief, the government offers the following reasons as to why, in its view, the SCA is a much better vehicle for obtaining prospective cell phone location data than the tracking device statute:

> **A. The Problem with § 3117: Lack of Compulsion**
> Both § 2703(c)(1)(A) and § 3117 require probable cause and utilization of Federal Rules of Criminal Procedure 41. A key distinction between § 3117 and § 2703 is that § 2703 allows officers to obtain an order directing a communication service provider to disclose specified information. See 18 U.S.C. § 2703(c) (stating that a governmental entity "may require a provider . . . to disclose" information when it obtains a warrant); . . . In contrast, § 3117 contains no provision for obtaining an order mandating third-party assistance in executing a warrant.
>
> **B. The Problem with § 3117: Impossible Installation**
> Title 18, United States Code, Section 3117 states:
>
> > If a court is empowered to issue a warrant or other order *for the installation of a mobile tracking device*, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.
>
> 18 U.S.C. § 3117 (emphasis added).
> Tracking or "homing" devices are physically installed on the property of another. For cell phones, the device itself has attributes of a tracker, but such tracking attributes are not "installed" by the Government. Unlike "homing" devices, beepers, or trackers, a cell phone is not a government installed device. Cell phones are carried (usually in a person's pocket or purse) and used voluntarily. Distinct from the execution of a warrant for a physical tracking device, however, execution of a prospective geolocation information warrant requires no governmental intrusion for installation of a device. Provisions of § 3117, for the installation of a tracking device, are inapplicable to prospective geolocation information warrants.

C. The Problem with § 3117: Inability to Determine Jurisdiction

Under § 3117, jurisdiction is based on the location of installation. If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction. Assuming arguendo that an "installation" is occurring, problems arise when deciding where installation is occurring. Whether installation is occurring at the location of the provider, or the location of the cell phone becomes an issue. Further compounding the problem, agents cannot determine the location of a cell phone at the moment of this "installation." Agents need a warrant to determine the location of the cell phone, but according to § 3117 they must know the location of the cell phone in order to obtain a warrant.

In support of this argument, the government offers the following practical example of the difficulties in proceeding under the Tracking Device Statute.

D. Practical Application

In December 2013, a bank robbery took place in Tupelo, Mississippi, and one police officer was murdered and another was critically wounded. Law enforcement determined that the same unidentified person, wearing the same clothing and driving the same vehicle, robbed a bank in Atlanta, Georgia, the day before.

The Government obtained cell tower information located near the Atlanta bank, along transportation routes between Atlanta and Tupelo, near the Tupelo bank, and near the location where the officers were shot. Based on this information, the Government identified a cell number that consistently communicated with towers in all the above referenced locations at pertinent times. However, by the time the Government determined this information, the perpetrator's whereabouts were still unknown. There was probable cause to acquire a § 2703(c) warrant, and time was of the essence.

According to § 3117, only a court in the jurisdiction where the phone is located can issue the warrant. In the aforementioned Tupelo bank robbery case, law enforcement had no idea where the cell phone is located, but apprehension of a violent killer obviously was of paramount concern.

However, § 2703 permitted the issuance of the warrant for geolocation information without regard to the location of the cell phone. In fact, the records obtained indicated that the cell phone was in Oklahoma. This information assisted Oklahoma law enforcement in the recovery of evidence tying the suspect to the Atlanta and Tupelo bank robberies. Ultimately, the suspect was killed in a shootout with officers in Phoenix, Arizona. Under a § 3117 analysis, the

> Government would have been unable to obtain a warrant for the location information; thus demonstrating why 2703(c) is the most obvious and practical statutory mechanism.

[Government's brief at 14-16].

The reasons which the government provides above do, in fact, suggest to this court that the SCA is, mechanically speaking, a superior statutory vehicle for obtaining prospective cell phone data from a provider than the Tracking Device Statute is. In response to the government's argument, the Federal Public Defender argues that the first two "problems" quoted above, i.e. those relating to compulsion and installation, are unlikely to actually prevent enforcement of an order under § 3117. It may well be true that a cell phone provider would likely comply with any order under § 3117, and it may also be true that the statute's seemingly inapplicable language regarding "installation" would not, as a practical matter, prevent enforcement of any order. At the same time, the issues raised by the government do serve as an indication that the SCA is better suited mechanically for the physical acts being mandated in this context than § 3117 is.

If the act of enforcing a warrant for production of cell phone location data can be analogized to hammering a nail, then the SCA is the statutory tool which looks, to this court at least, very much like a hammer. Conversely, § 3117, with its design centered around the physical "installation" of tracking devices on vehicles and its procedural and jurisdictional requirements applicable to that context, seems more like a wrench. Given that, in this case, this court is confident that the Fourth Amendment rights of defendants will be protected regardless, it sees no good reason to require the government to attempt to hammer a nail with a wrench. The SCA is specifically designed to compel third parties in the possession of cell phone data to provide that information to the government, pursuant to a court order or warrant. That is what the government is seeking to do in this case. Mechanically speaking, the fact that prospective,

rather than historical cell phone data is sought, appears to be of little moment in the context of a technology in which cell phone data is instantly transmitted to and recorded by phone companies.

This court's impression is that the government's most strenuous objection to § 3117 is the third one which it has raised, i.e. the one relating to uncertain jurisdiction. Significantly, the public defender appears to concede in its brief that this issue does present a real and practical obstacle to enforcement. For example, at one point in its brief, the public defender writes that "under § 3117(a), the cell phone must be present within the Northern District and satisfy the *in rem* jurisdiction requirement posed by the statute and a Rule 41 warrant based upon probable cause should be required." Later in its brief, the public defender writes that:

> [T]he prosecution argues that it will be difficult for their agency to determine jurisdiction. While this may be true, this is not a legal argument. The Constitution and Rules of Criminal Procedure must be followed.

In so arguing, the public defender misconstrues the government's position in this case.

Once again, the government is seeking a warrant based upon probable cause in this case, and, as Judge Alexander noted in her order, it has specifically invoked Rule 41 in doing so. Accordingly, this court views the government's actions in this case as being consistent with both the Constitution and the Rules of Criminal Procedure, even under the most pro-defendant interpretations of the uncertain law in this context. Moreover, this court can discern no good reason why Congress would have wanted to place seemingly arbitrary statutory obstacles to enforcement in the cell phone data context, once relevant constitutional concerns have been addressed. It seems clear that the practical difficulties in applying § 3117 to cell phone providers are real, and those difficulties might well lead to very unfortunate results in a particular case. Assume, for example a hypothetical involving attempts to locate a kidnapper who had taken a

child outside of a particular judicial district. Under these circumstances, this court doubts that any judge would hesitate to require that cell phone data be produced, but the admitted jurisdictional issues in this context might well cause delays in finding a judge with jurisdiction to enter such an order. Such delays might well lead to tragic results, in a particular case.

In this district (or at least in this case), the U.S. Attorney appears to have made a commendable decision to err on the side of protecting the Fourth Amendment rights of defendants, pending clarification regarding the applicable constitutional standards in the prospective cell phone data context.[3] The government could have chosen, as most U.S. Attorneys seem to have done, to seek an order based on the more lenient standards of § 2703(d) and appeal any denial of such an application to this court, or, if necessary, to the Fifth Circuit. If the government had done so, it appears, in light of *In re Application of the U.S.*, that it would have had a quite reasonable possibility (if not probability) of success. The government elected instead to seek a more cautious and measured form of relief, and this court believes that it should be given credit for doing so. In cases where the government proceeds in good faith and elects to make such a measured request for relief, this court becomes more inclined to grant it. The government will therefore be authorized to seek a warrant pursuant to § 2703(c)(1)(A) and Rule 41, and this case will be remanded to the Magistrate Judge for a determination of 1) whether the government is able to demonstrate probable cause in this case and 2) if so, what the scope of any warrant authorizing prospective monitoring of cell phone location data should be.

[3]This court does not regard the government's decision to proceed under § 2703(c)(1)(A) in this case as being an irrevocable commitment to do so in future cases, since the legal standards in this context are evolving and may well give it cause to re-evaluate its approach. Indeed, it seems clear in light of *In re Application of the U.S.* that the government has every right to seek *historical* cell phone data based on § 2703(d)'s lesser standard, and it presumes that it would do so in an appropriate case.

It is therefore ordered that the government's appeal of the Magistrate Judge's February 10, 2015 order is granted, and this case is remanded for proceedings consistent with this opinion.

This the 30th day of March, 2015.

/s/ MICHAEL P. MILLS
UNITED STATES DISTRICT JUDGE
NORTHERN DISTRICT OF MISSISSIPPI